St Louis Catholic Academy, Newmarket

Part of Our Lady of Walsingham Catholic Multi Academy Trust

Christ at the Centre: Children at the Heart
Loving to Learn: Learning to Love

Online Safety Policy

Prepared by	***Sue Blakeley/ Kiri Wyatt***
Approved by the Committee/Governing body	*St. Louis Local Governing Body*
Approved by Chair of Governors	*Bethan Byrne*
Date approved	*September 2023*
Review date	*October 2025*

The aim of this policy is to supplement the OLOW IT Acceptable Use Policy at a local level with a focus on pupils. This does not supersede that policy

The use of technology has become a significant component of many safeguarding issues such as child sexual exploitation, radicalisation and sexual predation and technology often provides the platform that facilitates such harm.

It is essential that children are safeguarded from potentially harmful and inappropriate online material. The school adopts a whole school approach to online safety to protect and educate pupils and staff in their use of technology, and establishes mechanisms to identify, intervene in, and escalate any concerns as appropriate.

The online risks to children are considerable and ever evolving, but can be categorised into four areas:

Online safety issues can be categorised into four areas of risk:

- **Content**: being exposed to illegal, inappropriate or harmful content, for example, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, or radicalisation or extremism;
- **Contact**: being exposed to harmful online interaction with other users, for example, peer to peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes;
- **Conduct**: online behaviour that increases the likelihood of, or causes, harm, for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images, and online bullying); and
- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and/or financial scams. If staff feel that either they or pupils are at risk this should be reported to the Anti-Phishing Working Group (https://apwg.org/).

  The governing body will ensure that an annual review is undertaken of the school's approach to online safety including the school's filtering and monitoring provision, supported by an annual risk assessment that considers and reflects the risks pupils face online. The review should include a member of the senior leadership team, the DSL, the IT service provider and a governor.

  The school should ensure they have the appropriate level of security protection procedures in place in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. Guidance on cyber security including considerations can be found at Cyber security training for school staff - NCSC.GOV.UK

  The named governor for filtering and monitoring is Karen Varma.

  The named member of SLT for filtering and monitoring is Sue Blakeley assisted by Kiri Wyatt Computing Subject leader.

The school internet systems have two levels of filtering:

The broadband provision to the site is protected by firewall/filter - RM SafetyNet

The RM SafetyNet filtering service is designed to facilitate the effective provisioning of safeguarding in a school environment and meets legal mandates set out under the Prevent Duty and Keeping Children Safe Online.

While centrally managed and updated, the service also enables schools to block sites that they deem inappropriate using age and user groups. Schools can then generate activity reports from their RM SafetyNet portal. The solution defines and applies filtering policies to the following user groups:

- Key Stage 1 and Key Stage 2 students
- Teaching staff
- Office administration staff

There are some categories which are blocked and cannot be overridden by schools:

Legal and liability issue

- child abuse
- drugs
- intolerance
- piracy and copyright infringement
- pornography
- self-harm
- terrorism
- violence

Other content can be over ridden by the school at a local level. This is manged by the IT support. The filter blocks access to sites which contain:

- adult themes
- abortion
- adult sites
- adult entertainers
- alcohol and tobacco
- body-piercing and tattoos
- Criminal activity
- Fireworks
- Gambling
- Gore
- Naturism and nudism
- Non-pornographic nudity
- Restricted to adults
- Sexuality sites
- Weapons: Hunting and sporting
- Weapons: military

- Weapons: Personal weapons
- Image hosting : unmoderated
- Plagiarism
- Malware and Hacking
- Dating and companionship sites

Further advice can be found: https://www.rm.com/products/rm-safetynet

School uses Impero on the school's computers as a classroom management tool, which also filters content.

Both systems filter sites on keywords/content and also by the website address.

The school can select additional content to be blocked or released when risks are identified. This is actioned by the school IT support Paul Collen.

Monthly reports from Impero identify any attempted breaches. Activity reports from RM SafetyNet portal enable school to identify over-blocking.

Teachers can identify site access which has been prevented and which has inhibited learning. This should be raised with the filtering and monitoring lead and a review of the RM SafetyNet portal activity report undertaken to decide if a change is required.

TEACHING AND LEARNING

Why internet and digital communications are important

- The internet is an essential element in life for education, business, and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.

- Internet use is part of the curriculum and a necessary tool for staff and pupils.

- Pupils are taught correct internet use: what is acceptable and what is not.

- Pupils have supervised access to IT and the internet, during lessons and extra-curricular activities.

- Pupils are educated in the effective use of the internet via Online Safety in Computing and RSHE lessons and through the Online Safety Team.

Pupils will be taught how to evaluate age appropriate apps and websites

- Staff will introduce pupils to a wide range of online media, apps and websites. They will be taught how to responsibly and independently choose which are most appropriate to their current task or requirement

- Pupils will be taught the rules and UK laws guiding our use of the internet, apps, websites and most importantly, social media. They will be informed that the majority of social media platforms whether websites or apps have a minimum legal age of 13 years and all others are from 16 years of age or older.

- Pupils will be shown strategies to identify, report and avoid the four areas of online danger identified by KCSIE (2023) – Content, Contact, Conduct and Commerce including phishing, grooming, cyberbullying, gambling and radicalisation.

MANAGING INTERNET ACCESS

E-mail and other forms of e-communication

- Staff will monitor use of Microsoft Teams when allowing the use of chat or between pupil communication.

- Pupils must not reveal personal details of themselves or others in electronic forms of communication, including social media, Microsoft Teams or in presentations of information.

- Staff to pupil communication may take place over Microsoft Teams regarding learning tasks set for homework or home learning – this is subject to monitoring through OLOW IT processes

- The sending of abusive, offensive, or inappropriate material is forbidden

Published content and the school website

- The only contact details published on the website are for the school (address, e-mail and telephone number). Staff or pupils' personal information is not published.

- The Headteacher takes overall editorial responsibility and ensures that content is accurate and appropriate.

Publishing photographs, images, and work

- Photographs that include pupils are selected carefully and do not enable individual pupils to be clearly identified by name.

- Pupils' full names are avoided on the school website or in communications between staff on e- mail. This is adhered to when teaching the pupils how to create blogs, vlogs or in presentation of information.

- Written permission from parents or carers is obtained before photographs or images of pupils are published and must be checked before use of said image.

- Parents receive information on image taking and publishing at the point of admission. This relates to school publications and outside publications, including use on the school website or on school social media.

- Pupils, parents and staff are advised on the safe use of social network spaces and the agreement on safe use is collected annually via Microsoft Forms.

Personal devices:

Many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school can sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. The school undertakes the following action:

- Pupil mobile phones are locked in safes at the start of each day.

- SMART watches can provide unfiltered access to the internet in school. Many have functions such as digital recording and the sending and receiving of messages. Such devices are not encouraged in school and if identified will be placed in the classroom safe to be returned at the end of the day.

- Children are not permitted to bring tablets or devices into school. The only permitted mobile devices used in school by pupils are those owned by the school for teaching and learning purposes.

Protecting personal data

- Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 2018 (GDPR)

- Pupils must agree to comply with the Acceptable Use Policy/Code of Conduct statement.

Handling Online Safety complaints

- Complaints of pupil internet misuse will be dealt with by the Online Safety Leader, who then reports this to the Designated Safeguarding Lead.

- Any pupil misuse of IT inside school and use of school IT services will be discussed with parents.

- Any complaint about staff misuse must be referred to the Headteacher, or in the case where the complaint relates to the Headteacher's misuse, this must be referred to the Trust IT Manager/Chair of Governors.

- Complaints of a child protection nature must be referred to the Designated Safeguarding Lead and dealt with in accordance with school child protection procedures.

- Pupils and parents are informed of the complaints procedure and this is published on the school website.

- Pupils and parents are informed of consequences for pupils' misuse of the school computers or the internet.

Community use of the internet

- All use of the school internet connection by community and other organisations shall be in accordance with OLOW Acceptable Use Policy

APPENDIX 1: EYFS / KS1 PUPIL AGREEMENT for Acceptable Use

This is how we stay safe when we use computers:

- I will ask a teacher if I want to use the computers, iPads, Interactive White Board, or other computing equipment.
- I will only use activities that a teacher has told or allowed me to use.
- I will take care of the computer and other computing equipment.
- I will ask for help from a teacher if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets or worries me on the screen.
- I know that I must be polite and take care with posting pictures or when I type something onto our Home learning page or class notebook.
- I will not meet other pupils on our Home Learning Platform without a school adult.
- I must keep my passwords private to me and my parents or carers. I must not share other's passwords.

Pupil _____ Date_____

Parent/ Carer _____

APPENDIX 2: KS2 PUPIL AGREEMENT for Acceptable Use.

These Online Safety Rules help to protect students and the school by describing acceptable computer use.

- I know that the school rules apply to use of the internet.
- I will only use IT systems in school for learning tasks set by the teachers.
- I will not post pictures or personal information of or about my family or friends on the internet without permission. I will not upload pictures of family or friends to Microsoft Teams.
- I will store my learning in class folder. I will not access other's work or folders without their permission. I will show respect to others when using the Microsoft Teams chat for a learning task. I will not meet other pupils on Teams without a school adult.
- I will be responsible for my behaviour when using the internet. This includes resources I access and the language I use in communication with others.
- If I accidentally come across any material which is inappropriate, unpleasant or upsets me, I will report it to my teacher or teaching assistant immediately. I will not disseminate or save material that is inappropriate to other pupils.
- I will not download or install software or files from any source, personal or otherwise, including memory sticks, on to school computers or other technologies, as this might cause viruses or other damaging problems which could infect the school system.
- I will always respect the privacy and ownership of others' work on-line including copying others' writing or images to present as my own.
- I understand the school may monitor, record, and control my use of the school's computer systems and online learning, via Microsoft Teams and, if necessary, report any misuse of the systems to other appropriate people.
- I understand that these rules are designed to keep me safe and that accept that I will only be allowed to use the school equipment and systems by following the rules.
- I will not use a personal device such as phone, smartwatch or tablet on school grounds and agree to place such devices in the care of the school whilst I am at school. I understand that they will be stored securely.

Pupil name:

Pupil signature: **Date:**

APPENDIX 3: PARENTAL FORM for Acceptable Use of Computing and Internet Services in Education Agreement

Parent / guardian name:……

Pupil name: …… Class: ……..

- As the parent or legal guardian of the above pupil(s), I grant permission for my child to have supervised access to use the internet, the Home Learning via Microsoft Teams and other IT facilities at school.
- I know that my child has signed a form to confirm that they will keep to the school's rules for responsible ICT use, outlined in the Online Safety Policy/Code of Conduct.
- I also understand that my son/daughter will be informed, as to the safety of new technologies or strategies.
- I know that the latest copy of the Acceptable Use Policy/Online Safety Policy is available on the School Website.
- I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, a monitored Home Learning platform and employing appropriate teaching practices and teaching online safety skills to pupils.
- I will not allow my child to bring in a mobile phone to school without permission. If permission is granted, the device will then be stored securely during the school day. The school cannot accept any responsibility for any loss/damage that may occur. I understand that the school can check my child's computer files and the internet sites they visit.
- I will not allow my child to bring devices such as tablets, internet enabled SMART watches or laptops into school.
- I understand that my child is not allowed to download or upload files at school from any source, including memory sticks, without permission, as these may contain unseen viruses or other damaging problems which could infect the school ICT system. I also know that the school may contact me if there are concerns about my son/daughter's online safety and online behaviour, including use of social media.
- I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

Parent's signature:…… Date:…….